

Information Protection Centers - An Organizational Approach to Security

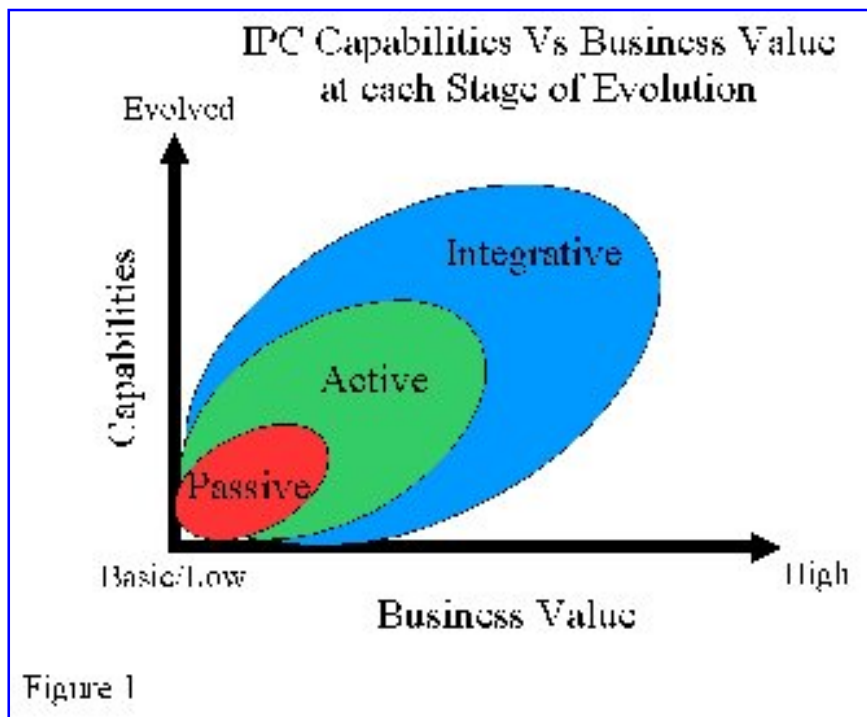
Andrew Mackie 2000-05-11

An organization connecting to the Internet without a comprehensive program of information protection is like a person without an immune system leaving their protective bubble-at some time they will come in contact with something that will harm or kill.

Most managers are not aware of the risks. They find the issues too esoteric and leave them to their technical staff to handle. Since they don't see security delivering a return on investment they don't want to throw a lot of resources (people, money) at it. Security is appropriately addressed only when it is considered vital to the business. The approaches that are provided in this focus area can be used to make security more directly supportive of your organization's business.

An IPC is a means to achieve this alignment. It is a name for an entity that carries out a wide spectrum of security activities and services necessary to secure an organization. Some of these activities may already be carried out independently or in loose coordination across the organizational structure. The IPC can start as a formal working group or virtual collaboration of the same people. What is important is that the group evolves to be a new functional unit with the blessing of senior management, both on the technical and business side. This will require a coordinated effort of service delivery and a communications campaign.

A good communications strategy is vital. Since security often has a negative image (gets in the way, costly, complex), the IPC is promoted as a centre of security excellence which delivers a range of security services. Solutions are offered along with the skills to implement those solutions. This usually overcomes resistance. Of course the members of the IPC need to possess or rapidly build these skills in order to deliver on their promises. It is necessary to carefully control expectations and allow sufficient time to do quality work. The selection of highly capable IPC staff is important. The IPC will often need to show their value quickly so that it forms a reputation for delivering good results. This will improve their support from management and gain more cooperation from within the organization.



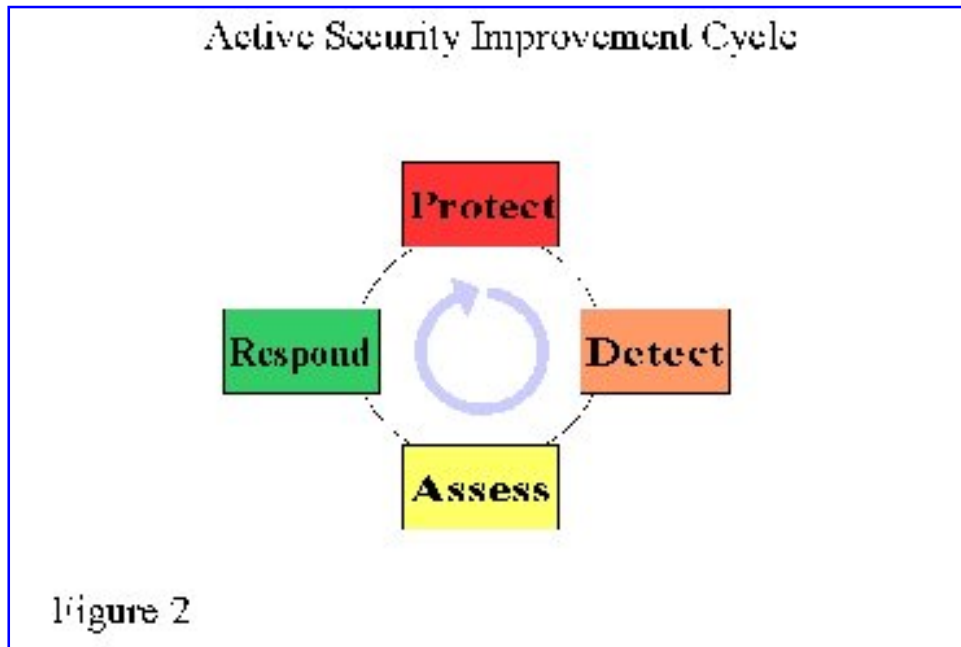
Evolution of Capabilities

The IPC model maps out an evolutionary progression from fundamental passive security practices into active security practices and eventually into a position of influence that integrates with the business side of the organization. The following diagram (figure 1) shows business value or impact on the performance of the organization increases with the increase in capabilities.

The IPC can start small and, as it gains recognition and support, take on more roles. It may not begin with the passive stage. Often it will start somewhere in the active stage with the group involved in managing firewall(s). Those performing such active security quickly recognize the value of an organizational security policy as they attempt to impose firewall controls. Without direction and support from senior management they can start with a strong set of policies and quickly find themselves fighting demands to open a variety of high risk services. If the IPC is to be effective it should ensure that the necessary policies are in place and compliance is being measured. Policy without measurement and enforcement is worse than no policy since it indicates that management does not have control.

The active security stage involves establishing automated policies, watching for violations in the logs, assessing the impact and responding to improve security where necessary. This protect-detect-assess-respond security cycle (figure 2, click to view larger image) seeks continuous improvement and is a "best practice" in highly evolved organizations. The IPC itself should

strive to achieve continuous improvement in its own operations. The [IPC Operations \(OPS\) Manual](#) has checklists that include such measurement and improvement practices.



If the IPC only carries out active security centered on the perimeter, then it is not addressing all of the organization's security needs. A comprehensive approach requires that the IPC move into the integrative stage where it works with the business to improve the selection of technology and assists developers in better integrating security within their business applications. One way to do this is to improve the security architecture by delivering secure infrastructure services (Virtual Private Networks, the new IPSec protocol standard, file and message encryption, Public Key Infrastructure, etc.).

Security Services at each Stage

Some tools, products and activities that may be used in support of IPC services at each stage are listed in the following table:

Evolutionary Stage	Improvement Cycle Phase	Tools, Products and Activities
Passive		Policy development, Audit checklists, Interviews, Threat and Risk Assessments
Active	Protect	Firewalls, Rules of Engagement, Vulnerability Analysis (VA) , Environmental scanning

Active	Detect	Intrusion Detection (ID), Tripwires, Viral scanning, Network mapping, Honeypots, Sandboxes
Active	Assess	Central collection of all available information (logs, vulnerabilities, threats, ID alerts, network maps, etc). Data mining of this combined information and assessment of the impact on the business, Triage, Escalation of operational vigilance
Active	Respond	Stop further attacks, Prevent any migration of an attacker, Record any evidence, Cleans the affected systems and Return to secure, operational state
Integrative		Selection of technologies (VPNs, IPSec, File encryption, PKI), Enforcement of standards, Preparation for next generation of applications

Details on the Passive, Active and Integrative Security Stages

The evolutionary stages of IPC are described in more detail in the following sections.

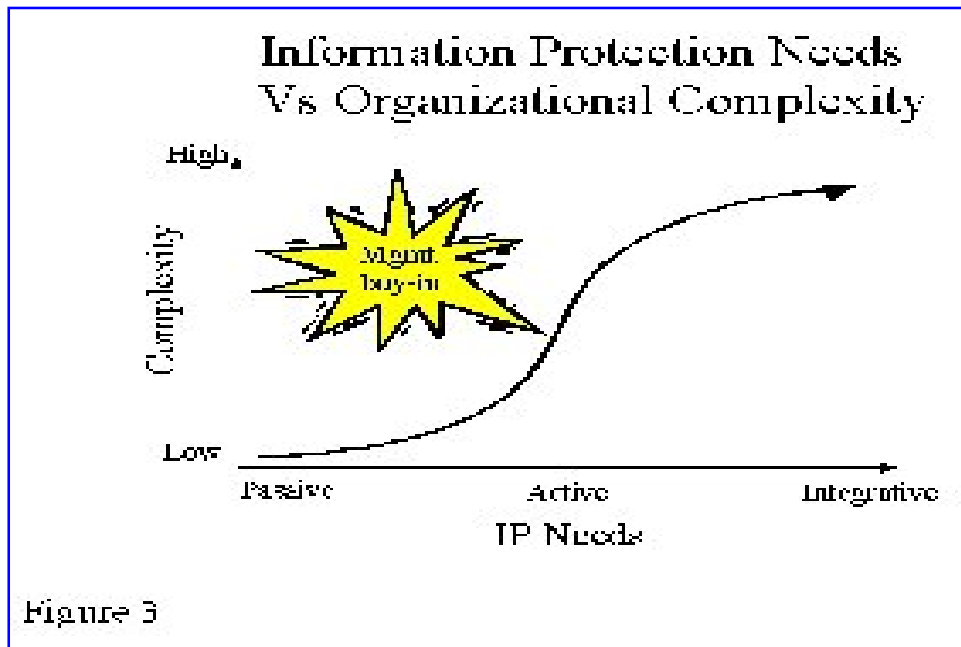
Passive Stage

Passive security is fundamental. Organizations need policies otherwise further security activities are not viable. Management must formally indicate whether security is important and what actions may be taken in the case of infractions. They then must back this up with audits for compliance and act to address non-compliance. Otherwise this policy, and likely others will have no effect and Management will not be in control. Securing such organizations can be challenging to say the least.

Other services the IPC can offer as part of passive security are security guidelines or advice and security awareness. Both of these are longer-term life-cycle efforts that will require periodic updating. The quality of these services will be improved as the IPC members gain experience, gather statistics and war stories and build their reputation.

Passive security was sufficient before organizations moved to networked systems. The security officer roles were mostly clerical and the only active security efforts were limited to auditing systems for compliance to some set of standards. As organizations moved to rely on distributed networked computers, ease of communications took precedence over security and control. This

opened a Pandora's Box of complex issues that require more active solutions. Organizations now need the equivalent of an immune system for their critical infrastructure if they are to survive. They need to put a variety of capabilities in place to be ready to face the increasing threats that they will face in the future. Their security needs to be active and fully integrated with their business operations. To accomplish this requires management buy-in (see figure 3, click to see larger image).



Active Security

The active stage of an IPC represents a security improvement cycle:

- protecting the organization while allowing effective business practices,
- analyzing the residual vulnerabilities,
- detecting any malicious or suspicious activities that may take advantage of the vulnerabilities, and
- assessing whether this represents a negative impact on the organization and responding in an appropriate manner.

This improvement cycle need not be limited to adjustments in the technology; it can extend to making adjustments to the organization's formal policies and awareness campaign if this helps to address security exposures.

Actively Protect

Setting up to do business securely on the Internet starts with a protective perimeter to establish controls on what can come into the organization. At this Protective stage the controls are intended to prevent bad things from happening. They automate policy enforcement, restricting by default and allowing only those services necessary to support the business activities. A variety of network layouts can be involved to maximize the controls and minimize the ways for unauthorized entry to the organization.

No amount of protection is absolute as long as there is connectivity into the organization. Firewalls are essentially sieves, so attacks can be staged against internal systems. The protection services of the IPC need to be extended to include vulnerability analysis (VA) and environmental scanning.

VA is a process that begins with a scan of all IP address ranges in the organization to detect active nodes. The VA then probes them to see what information or services could be used to stage an attack against them. The results of the scan become a baseline security profile. The IPC assesses the results, passes a report up to Management to raise their awareness of business risk and works with the system owners to address the exposures. The VA is repeated at least once a year. The results are measured against the previous baseline with the objective to achieve continuous improvement.

Environmental scanning means simply keeping connected to the many sources of vulnerability alerts. The Internet itself is the best source of these announcements. The idea is to identify threats that may impact your environment, increasing the business risk. Your organization's Y2K inventory of applications and operating systems can be used to determine if the vulnerability or new threat exposes the organization.

Integrity and control of the perimeter is vital. If there are unauthorized modems within the perimeter, there may be back doors for attack. Tools exist to search these out either by dialing in to detect answering modems or using network management tools to identify computers with multiple network interfaces.

Actively Detect

Once the IPC has protective services in effect, it can move into the Detective stage where it is looking for bad things that have happened, or are about to happen. This can be done using intrusion detection (ID), viral scanning, tripwires, network mapping, sandboxing and honeypots.

Intrusion detection (ID) can detect suspicious patterns of activities or known attack signatures on the network or on the computers themselves. Network ID usually relies on promiscuous sniffing of packets as they flow over a network subnet. Host-based ID looks for suspicious activities in operating system logs and may also do some analysis of network or other processor activities.

Viral scanning can be done on servers, on desktops and/or at the perimeter. The ideal is to catch bad things (email attachments, ftp file transfers, floppy transfers) as they come into the organization and before they get a chance to spread. Most current commercial scanners can automatically neutralize the virus. Many also detect popular trojan programs or other malicious or dangerous code.

Tripwires involve the calculation of mathematical fingerprints or hash codes for files. If this is done for all critical files and the results stored securely, then the files can be checked for changes. This integrity checking can accurately determine whether a system has been compromised or a trojan or back door program has been inserted.

Network mapping identifies what is on your network. Such a map is vital in establishing and maintaining the integrity of your security perimeter. Unless you are responsible for all network services, you probably don't know what the network looks like, where it goes and what it is connected to. You can't secure what you don't know. An accurate mapping is necessary to determine the access points to your organization's networks and whether they are all secured. With this map in hand you are now able to plan where best to fit intrusion detection and how to interpret the logged events.

Network mapping can be done manually if the network is small and well known. A simple diagram showing how things connect and indicating IP addresses can be sufficient. Larger networks are likely already mapped by those responsible for network support. Automated system management tools relying on the system network management protocol (snmp) are usually deployed to do trouble detection. These management frameworks are very costly and take a lot of effort so it is best to take advantage of these if they are already in place. If you need your own mapping tool then look at the new network management appliances that have appeared; these take less support.

Sandboxing is used to restrict the activities of imported code, usually downloaded as applets from the Internet. Since these applets often add useful or nifty features to web content it is

hard to impose strict filtering of these at the perimeter. Sandboxing is a compromise. It provides a controlled environment in which the downloaded code can run and it monitors activities to detect unauthorized access to system resources.

Honeypots are hosts that are made to look interesting and appealing to would be attackers. All activities are heavily logged. Elaborate honeypots build virtual electronic mazes that catch and hold the interest of an interloper. The logs from honeypots can be useful if the incident leads to prosecution.

Actively Assess

The tools and products provide raw data that is filled with false alarms (false positives). The data must be carefully assessed by consolidating all available logs, VA results, threat alerts, network maps and knowledge of filtering policies and business operations. If the data indicates that the organization is truly at risk or there is evidence that a compromise has occurred, or is taking place then an "attack" can be declared.

The assessment can indicate a priority of the incident based on impact to the organization. If the IPC is actively handling several incidents then the priority will assist in doing triage and deciding where to allocate resources. Central assessment of all logs and sensor data can indicate when there is a coordinated attack or signs of a build-up of activity requiring an increase in operational vigilance.

Some tools and products exist which accumulate data from a variety of sources and allow some automated analysis or data mining. The increased number of devices generating logs for review is creating a market demand for such automated collection and analysis so expect a lot of new products which will help in this area.

Actively Respond

If an "attack" has been determined then something must be done to stop further attacks, prevent any migration of an attacker, record any evidence, clean the affected systems and get operational as quickly and securely as possible. In simple incidents this may only require a change to firewall filtering or the application of a software patch. ID systems can include automated responses for the most obvious malicious activities. In major attacks which successfully compromise systems the network attachment may have to be cut allowing each

affected system to be isolated before evidence can be altered or further systems compromised.

It is best to do a full disk image backup prior to any attempt to investigate the attacker's activities on a system. Any tripwire and VA results for the system can help find out what may have been changed and how the system may have been compromised in the first place. It is good to use the latest probing tools to see what new vulnerabilities the system may have. The main objective is to get the system operational as quickly as possible but also ensure that the same thing doesn't happen again.

Integrative Stage

The Integrative stage is the highest evolutionary achievement of an IPC. The integrative stage is where improvements are made to the organization's architecture (technology, applications and processes) to enhance the effectiveness of its overall security. At the integrative stage the IPC's improvement cycle encompasses the entire range of passive, active and integrative efforts. This is best achieved where the IPC can influence technology selection and how it is deployed.

The IPC does not have to reach this level of effectiveness. It can operate successfully at the other stages, enhancing security and delivering value. Integration within the architectural decision making process of the organization brings the IPC closer to the business side of the organization. Until it reaches this level it will always be attempting to mitigate risk after the business decisions have been made.

Long Term Growth

An effective IPC must select some appropriate subset of services that they can deliver with the people, time and tools they can afford. The ideal strategy is to start small and agile, relying on the expertise of team members. Provide assistance in solving business problems: clean up incidents, bring in secure remote access technology, secure laptop data. Once the IPC reputation has been established then use this to leverage more resources in return for delivering more services. Follow this model of growth until a size appropriate to the size and value of the business.

We hope this article has helped to describe the Information Protection strategy behind the IPC framework. The objective is to make an organization's security resources sufficiently agile that

they can act as an immune system, fending off attacks. Internet threats are becoming increasingly malicious. Political agendas, simple point-and-click denial of service tools and creative mutations of Chernobyl, BubbleBoy and the LoveBug make it vital that a healthy and responsive incident handling capability be developed within and across all organizations.

Andrew Mackie installed active security technology and formed an Incident Response Team in 1997. He did this while working as Security Architect for an infrastructure upgrade of Canada's Communications Security Establishment. This past year he built and led Manitoba's Information Protection Centre (IPC) and assisted the National Subcommittee on Information Protection in developing a national IPC initiative. Mr. Mackie now heads his own [TrustworthEServices](#) security consulting company.

Relevant Links

[Information Protection Center \(IPC\)](#)

Andrew Mackie

[Privacy Statement](#)

Copyright 2006, SecurityFocus